AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph beginning on page 2, line 42 (last paragraph) as follows:

In order to achieve these objectives, an exemplary embodiment of the present invention is a card settlement method wherein a portable electronic device having a fingerprint sensor is connected to a card company's card management ~~device~~ system via a communication terminal for card settlement of a commodity purchase charge or the like; it is characterized by comprising:

Please amend the paragraphs beginning on page 3, line 12 (third full paragraph) as follows:

A transmission step wherein the electronically signed transmission data is sent from the side of the portable electronic device having a fingerprint sensor to the card management ~~device~~ system, and

A decryption and settlement processing step wherein the card management ~~device~~ system decrypts the electronically signed transmission data using a transmission secret key paired with the transmission public key and processes the settlement.

Preferably, the fingerprint data and the card information of the portable electronic device having a fingerprint sensor are registered in a state in which they are encrypted by a storage public key provided [[from]] by the card management ~~device-side~~ system. In this case, decryption using the storage secret key paired with the storage public key may be performed in the step of decrypting the card settlement data at the card management ~~device~~ system.

Preferably, the card management ~~device~~ system stores and retains the received card settlement data for a predetermined time period.

Next, the card management ~~device~~ system preferably updates the transmission public key and the storage public key registered in the portable electronic device having a fingerprint sensor

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

as required. In this case, the portable electronic device having a fingerprint sensor may perform processing to replace the registered card information and fingerprint data with card information and fingerprint data that were encrypted using the updated storage public key.

Another exemplary embodiment of the present invention is a portable electronic device having a fingerprint sensor that connects to a card company's card management ~~device~~ system via a communication terminal for card settlement of a commodity purchase charge or the like; it is characterized by comprising:

Please amend the paragraph beginning on page 3, line 36 (tenth full paragraph) as follows:

The storage unit stores the transmission public key and storage public key provided from the card management ~~device-side~~ system, card information for card settlement provided to the owner of the portable electronic device having a fingerprint sensor, master fingerprint data, and a personal encryption key,

Please amend the paragraphs beginning on page 4, line 1 (first paragraph) as follows:

A transmission data generation and transmission means for encrypting commodity order information and card information using the transmission public key and generating transmission data, for electronically signing the transmission data using the personal encryption key, and for sending the electronically signed transmission data to the card management ~~device~~ system.

Here, the processor can be constituted to comprise a master fingerprint data registration means so that when it receives a registration permission signal from the card management ~~device~~ system, it reads master fingerprint data using the fingerprint sensor and registers it. In this case,

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

the personal encryption key generation means preferably generates the personal encryption key using the fingerprint data read when reading the master fingerprint data.

Please amend the paragraph beginning on page 4, line 27 (eighth paragraph) as follows:

Next, an exemplary embodiment of the present invention is a card settlement system that connects a portable electronic device having a fingerprint sensor to a card company's card management ~~device~~ system via a communication terminal and performs card settlement of commodity purchase charges, etc.; it is characterized in that:

Please amend the paragraphs beginning on page 4, line 39 (twelfth paragraph) as follows:

A transmission means for sending the electronically signed transmission data to the card management ~~device~~ system;

The card management ~~device~~ system comprises:

Please amend the paragraphs beginning on page 5, line 1 (first paragraph) as follows:

Preferably, the fingerprint data and card information of the portable electronic device having a fingerprint sensor are registered in a state in which they are encrypted by a storage public key provided [[from]] by the card management ~~device side~~ system. The card management ~~device's~~ system's decryption means preferably decrypts using a storage secret key paired with the storage public key.

Preferably, the card management ~~device~~ system comprises a storage means for storing and retaining the received card settlement data for a predetermined time period.

In addition, the card management ~~device~~ system preferably comprises an encryption key update means for updating the transmission public key and the storage public key registered in

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

the portable electronic device having a fingerprint sensor. In this case, the portable electronic device having a fingerprint sensor preferably comprises a data update means for replacing the registered card information and fingerprint data with card information and fingerprint data that was encrypted using the updated storage public key.

Please amend the paragraphs beginning on page 5, line 27 (twelfth paragraph) as follows:

FIGURE 1 is a block diagram showing the structure of one example of a card settlement system, and FIGURE 2 is a block diagram of a portable electronic device having a fingerprint sensor. A card settlement system 1 includes a card management ~~device~~ system 3 installed at the card company 2 side, a portable electronic device 5 having a fingerprint sensor provided to an owner 4 of a settlement card such as a credit card, etc. by the card management company 2, and a communication terminal 8 such as a personal computer 6 or card settlement terminal 7 capable of connecting the portable electronic device 5 having a fingerprint sensor. Also, there is a network such as the Internet 9 capable of connecting the portable electronic device 5 having a fingerprint sensor and the card management ~~device~~ system 3.

The portable electronic device 5 having a fingerprint sensor is issued by the card company 2 together with a credit card to a person who applies for a card. When the card applicant receives the portable electronic device 5 having a fingerprint sensor, the applicant accesses the card ~~company 2's~~ company's card management ~~device~~ system 3 via the communication terminal 8 and the Internet 9 and does a registration procedure to utilize the credit card. When the registration procedure is complete, it becomes possible to pay a charge for a commodity purchased at an online shipping site 10 on the Internet 9 through card settlement using the portable electronic device 5 having a fingerprint sensor.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Please amend the paragraphs beginning on page 6, line 5 (second paragraph) as follows:

Written into the nonvolatile memory 53 are a public key Kp1 for encrypting and storing card information (hereinafter "storage public key") and a public key Kp2 for additionally encrypting the encrypted card information and sending it to the card management ~~device~~ system 3 (hereinafter "transmission public key"). Also written into the memory are the card owner's own secret key Ks3 and public key Kp3 generated using fingerprint data. For example, this sort of secret key and public key can be generated using fingerprint data noise. The card owner's master fingerprint data 11 is also registered.

Meanwhile, the card ~~company 2's~~ company's card management ~~device~~ system 3 includes a front server 31 that is a web server, a settlement server 32, an archive server 33, and a database 34 for storing the card transaction history, etc. The front server 31 decrypts information received via the Internet 9 and passes it to the settlement server 32. The front server 31 holds the transmission secret key Ks2 paired with the transmission public key Kp2 held by the portable electronic device 5 having a fingerprint sensor and the storage secret key Ks1 paired with the storage public key Kp1. Received information is decrypted using these secret keys Ks1 and Ks2. Furthermore, in this example the public key and encryption key and electronic signature systems all conform to the specifications of PKI.X.509.

Please amend the paragraphs beginning on page 6, line 35 (eleventh paragraph) as follows:

As soon as the applicant receives the portable electronic device 5 having a fingerprint sensor and the credit card from the card company 2, the applicant connects the portable electronic device 5 having a fingerprint sensor to a communication terminal 8 such as a personal computer 6 (arrow 103). Then the applicant accesses the URL indicated by the card company 2

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

via the communication terminal 8 and the Internet 9, establishes communication with the card management ~~device 3's~~ system's front server 31 (arrow 104), and issues a registration request signal (activation request) (arrow 105).

Subsequently, the Social Security number or driver's license number reported when the card applicant requested a card are checked, and the secret question (a pet's name, mother's maiden name, etc.) is asked on the web (confirmation of identity identification information), and the identity is confirmed (arrow 106). When the card company's front server 31 confirms that the question answerer is truly the card applicant, the card ~~company 2's~~ company's front server 31 sends a registration permission signal (activation permission signal) to initiate fingerprint data registration to the portable electronic device 5 having a fingerprint sensor (arrow 107). As a result, the card applicant is formally registered as a card member 4 at the card company 2 side.

Please amend the paragraphs beginning on page 7, line 10 (second full paragraph) as follows:

When the portable electronic device 5 having a fingerprint sensor confirms that the required fingerprint data is in order, the fingerprint data is registered in the nonvolatile memory as master fingerprint data 11 (arrow 109). At the same time, the card ~~member 4's~~ member's personal secret key Ks3 and personal public key Kp3 are generated using the fingerprint data. For example, the card ~~member 4's~~ member's personal secret key Ks3 and personal public key Kp3 are generated using the noise that accompanies the fingerprint data when acquiring the fingerprint data. These keys are utilized for creating an electronic certificate.

Please amend the paragraphs beginning on page 7, line 26 (sixth full paragraph) as follows:

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

When settling the purchase charge for the ordered commodity, instead of entering a card number for settlement the fingerprint sensor 51 of the portable electronic device (token) 5 having a fingerprint sensor scans the finger corresponding to the registered fingerprint. If the master fingerprint data 11 stored in the nonvolatile memory 53 matches the fingerprint data of the scanned finger, the portable electronic device 5 having a fingerprint sensor recognizes that the card member 4 is doing a settlement transaction, and uses the transmission encryption key Kp2 to encrypt the card information 12 encrypted by the storage encryption key Kp1 written by the card company 2 and information 13 pertaining to the purchased commodity (commodity order information). At the same time this is electronically signed with the card ~~member 4's~~ member's personal public key Kp3 and secret key Ks3 (arrow 125). Then the encrypted and electronically signed transmission data (transaction data with an electronic signature) 14 is sent via the Internet 9 to the card ~~company 2's~~ company's front server 31 (arrow 126). The significance of an electronic signature is to prevent the card member 4 from not confirming the settlement transaction.

When the card ~~company 2's~~ company's front server 31 receives the electronically signed transaction data 14 it decrypts it with the secret key Ks2 paired with the transmission encryption key Kp2, and additionally decrypts it with the secret key Ks1 paired with the storage encryption key Kp1, and decrypts the card information 12 (block 127). Then the settlement server 32 is asked for settlement (arrow 128). That is, processing shifts to a settlement process that is the same as a conventional one. Also, the electronically signed transaction data 14 that was sent can be kept in a long-term archive in order to prevent the card member 4 from denying the settlement transaction, etc. (arrows 131, 132).

Thus in the card settlement system 1 of this example an electronic signature is applied using the individual's secret key Ks3 generated in the portable electronic device 5 having a

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

fingerprint sensor, so this determines that the card member himself, who is the owner of the registered fingerprint, used the portable electronic device 5 having a fingerprint sensor and did a settlement transaction. Also, the encrypted data is decrypted using the ~~card company 2's front server 31's~~ card company's front server's secret keys Ks1 and Ks2, thereby determining that the data itself was sent from the portable electronic device 5 having a fingerprint sensor that was issued by the card company.

Please amend the paragraphs beginning on page 8, line 14 (third full paragraph) as follows:

If the portable electronic device 5 having a fingerprint sensor is connected to the Internet 9 via the communication terminal 8 such as a personal computer 6, etc., it communicates online with the card ~~company 2's~~ company's settlement server 32. Therefore it is possible for the card company 2 to change the storage public key Kp1 and the transmission public key Kp2 written to the portable electronic device 5 having a fingerprint sensor when necessary. By doing so, it is possible to additionally enhance the security of the encryption keys used for encryption. Furthermore, when the encryption keys are revised, the data written in the nonvolatile memory 53 needs to be updated by data that was encrypted using the new encryption keys.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100